Password Policy

1 Version history details and author

1.0 05/10/2010 Completed for distribution Jo White
2.0 27/10/2010 Approved by Information Governance Group Jo White
3.0 25/10/2011 Reviewed by Information Governance Group Jo White
4.0 28/11/2012 Reviewed by Information Governance Group Jo White
5.0 13/01/2014 Reviewed by Information Governance Group Jo White
6.0 03/11/2014 Reviewed by Information Governance Group Jo White
7.0 09/05/2016 Reviewed by Information Governance Group Jo White
8.0 12/06/2017 Reviewed by Information Governance Group. Jo White.
9.0 08/05/2018 Reviewed by Information Governance Group. Amendments made to supply of passwords to new starters and account lockout thresholds. Jo White
10.0 08/07/2019 Reviewed by Information Governance Group. Password length increased to 12 characters, frequency of change to 90 days from 42. Jo White
11.0 09/03/2021 Reviewed by Information Governance Group. Password frequency changed to 180 days. Jo White
12.0 06/08/2021 Reviewed by Information Governance Group. Jo White
13.0 04/10/2022 Reviewed by Information Governance Group. Removed references to office. Addition of group logon advice. Jo White
14.0 10/10/2023 Reviewed by Information Governance Group. ISO27001 controls updated. Jo White
15.0 12/11/2024 Reviewed by Information Governance Group. MFA to be used where possible. Jo Williams
16.0 09/12/2025 Reviewed by Information Governance Group. MFA to be mandatory. Windows Hello added. Jo Williams

This document has been prepared using the following ISO27001:2022 standard controls as reference:

A.5.15 - Access control
A.5.16 - Identity management
A.5.17 - Authentication information
A.5.18 – Access rights
A.8.5 – Secure authentication

2 Introduction

Passwords are an essential element of the Council's network security - they are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Council's entire corporate network. As such, all Derbyshire County Council employees, elected members, partner agencies, contractors, volunteers and vendors with access to Council systems are responsible for taking the appropriate steps, as outlined below, to select, use and secure their passwords.

3 Purpose

The purpose of this policy is to establish a standard for the creation of strong passwords, the protection of those passwords and the frequency of change across all Information and Communication Technologies (ICT) related systems throughout the Council.

4 Scope

This policy applies to all employees, elected members, contractors, volunteers, vendors, agency staff and partner agencies who:

- have or are responsible for any network account or resources (or any form of access that supports or requires a password) on any system that resides at any Council facility.
- have access to the Council's data network.
- store any personal, sensitive or confidential Council information.

5 Policy Statement

The continual reliance on IT systems, requires that effective password controls are in place to ensure that the integrity of all system/access logon accounts used across the Council is maintained. The following procedures and practices must be followed to ensure the security and integrity of these accounts.

- All users must ensure that their password is not divulged or shared with anyone else.
- All users **must not** create passwords that fall into the category of weak passwords under the construction guidelines.
- All users must not write down and store passwords.
- Passwords must not be inserted into email messages or other forms of electronic communication with the exception of some systems/processes which may require automatically generated temporary passwords to be sent. **Temporary passwords must be changed as soon as possible.**
- Those users adopting 'Windows Hello' for business must not share any PINs they may use for 'Windows Hello'.
- All ICT devices which may require local logon privileges for configuration and maintenance i.e. Printers, network switches, routers, SAN appliances etc. must all have the built-in default admin (or equivalent) account password changed in line with the guidelines of this policy wherever possible. Consideration should be given in the use of Multi-Factor Authentication (MFA) wherever possible or appropriate
- All ICT systems should:
    - Support individual user authentication – providing for identification of specific users and not just groups. Where this cannot be achieved (e.g. access to services designed for shared use) a shared password must be stored in a single designated secure repository, accessible only to the users who need it. These password sharing arrangements must be regularly reviewed.

- Prevent the storing of passwords in clear text or in any easily reversible form
- Provide for management of specific roles and functions within a system enabling delegation of tasks to individuals
- Not contain or utilise embedded (hard-coded) passwords – these are passwords which are “fixed” (saved) on a computer or device and are often “hidden” from view. Embedded passwords can be used as a “back door” to computers and systems and must be prevented.
- Use access control procedures, which apply to both operational and test systems equally.

This policy relates to both the internal and external Derbyshire domains to which employees, elected members, contractors, volunteers, vendors and partner agencies logon. Specific configuration of enforced password policies for each domain is as follows:

5.1 Internal Users

The Council’s main network enables user logons and authentication. It is also the security boundary for the majority of systems in use and accessed by Council employees, elected members, partner agencies, contractors, volunteers and vendors.

Password configuration enforced by the default domain group policy for this domain:

- Minimum password length **12** characters
- Users are prompted to change their password at first logon and **7** days prior to the existing one expiring.
- Passwords must meet complexity requirements – this forces the use of passwords which must contain at least four of the following five elements:
  - Numeric – (0-9)
  - Uppercase – (A-Z)
  - Lowercase – (a-z)
  - Special Characters (?,!, @, #, %, etc…)
  - Spaces

5.2 External users

This area services external (3rd party) connections to the Council’s network and facilitates external user logons and authentication. It is the security boundary placed between the Internet and the Council’s internal network. This domain boundary is used to contain user account logons for various parties including software support and interim access.

Password configuration enforced by the default domain group policy for this domain:

- Minimum password length **12** characters
- Password must meet complexity requirements – detailed as above **5.1**

All externally procured software must satisfy the requirement of this policy. The Supplier Information Security Policyalso defines when externally procured software and applications (Apps) must use Multi-Factor Authentication (MFA) and/or single sign on where possible.

5.3 Password Configuration Settings

Detailed password configuration settings for IT Systems or applications purchased by the Council will be supplied as part of the procurement process, where applicable.

5.4 Multi-factor authentication (MFA).

To protect Council resources and data in accordance with Zero Trust principles, all employees, elected members, contractors, volunteers, vendors, agency staff and partner agencies must authenticate using MFA.

As part of the principle of least privilege access, the Council enforces MFA as a key control to support conditional and risk-based access.

This password policy specifically applies to the “Something You Know” factor within MFA.

6 Responsibilities

Implementation and adherence to this policy is the responsibility of all Council employees, elected members, partner agencies, contractors, volunteers and vendors working for the Council. It is important that every employee takes seriously, the use, protection and integrity of their own password/s or any other system password/s which they may be privy to from time to time and to encourage, guide and inform staff wherever possible for those who are responsible for the supervision of others.

7 Compliance with legal and contractual obligations

- The Data Protection Act (2018) requires that personal data be kept secure against unauthorised access or disclosure. The password is part of the security environment.
- The Computer Misuse Act (1990) covers unauthorised access to computer systems, including the use of another person’s identity. If a user “lends” their account and password to another individual who then breaches the Computer Misuse Act, both the individuals concerned could be deemed to have committed an offence.

8 Breaches of Policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council’s security procedures and policies.
All employees, elected members, partner agencies, contractors, volunteers and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council’s Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council.

In the case of third party vendors, consultants or contractors, non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Council’s ICT systems or network results from the non-compliance, the Council will consider legal action against the third party. The Council will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. In the case of an individual the matter may be dealt with under the disciplinary process.

9 General Password Construction Guidelines

Passwords are used for various purposes at Derbyshire County Council. Examples of some of the more common uses include: user level accounts, web accounts, email accounts, local access to ICT devices such as routers, printers etc. All staff should be aware of how to construct and select strong passwords.

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits, punctuation and special characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least twelve alphanumeric characters long.
- Are **not a word in any language**, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored online. Try to create passwords that can be easily remembered.

Poor, weak passwords have the following characteristics and **must not** be used:

- The password contains less than twelve characters and doesn't include any special characters or numbers
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Repetition such as mmmmmmmm1
    - Hashtags and profile names ie anything in the public domain
    - Common passphrases found on the internet such as nursery rhymes, song names, slogans etc.
    - Word or number patterns like aaabbbcc, zyxwvuts, 123321, etc.
    - Keyboard sequences like qwerty, asdfghjk , zxcvbnm, etc
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Creating Passwords using Passphrases

Using passphrases is a good way of constructing strong passwords and helps with remembering them. Passwords constructed in this way, will typically consist of letters, numbers and special characters which are used to represent the words or meaning of a phrase. The following example describes this process:

Example

Step 1 – Choose a phrase – for example: ***'I catch the number 14 bus on Fridays'***

Step 2 – Use the first character of each word: I c t n 14 b o f

Step 3 – Mix with lower and uppercase letters: **iCTn14bOf**

Step 4 – Incorporate special characters (such as !@#$%^&*()_+|~-=\`{}[]:";'<>?,./) and numbers to increase complexity. Using this method, the final password could be:

i*CTn#14bOf5

N.B. Incorporate special characters and numbers into your password in a way which helps you to remember where they should be e.g. could be after every 2nd, 4th, or 5th letter – or a similar 'system' which is meaningful to you.

Basically, the more letters, special characters and numbers used and the longer the password containing these is, the stronger the password will be.

IMPORTANT: The above passphrase/password is an example and must NOT be used.

Password Protection Standards

- Do not use the same password you use for Council accounts as for other non-Council access (e.g., personal ISP account, personal banking, online shopping etc.).

- Do not share Council passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Council information.

- For new starters to obtain their initial network login password, the new starter is instructed by their line manager to contact the ICT Service Desk to verbally provide a 'onetime' use password which must be reset upon first login.

- Where a member of staff forgets their current network password this can be reset by contacting the ICT Service Desk. Following a security check, the ICT Service Desk staff will reset existing users' network password by verbally providing the user with a 'onetime' use password.

List of "**Don'ts**":

- Don't reveal a password over the phone to ANYONE - unless relaying information on temporary passwords which are changed immediately
- Don't write passwords down and store them anywhere in your office
- Don't reveal a password in an email message - unless relaying information on temporary passwords which are changed immediately
- Don't reveal a password to your line manager
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on holiday

Additional Information

- If someone demands a password, refer them to this document and request that they call the Service Desk.

- Do not use the "Remember Password" feature of applications (e.g., Internet Explorer, SAP etc…).

- Do not store passwords in a file on ANY computer system (including mobile devices or similar) without encryption.

- Change passwords at least once every 180 days (with the exception of system-level passwords which must be changed quarterly). The recommended change interval is every four months.

- If an account or password is suspected to have been compromised, report the incident as soon as possible to the Service Desk or via one of the other methods as described in the Council's Security Incident Management Policy and Procedures. Immediately change any/all passwords which may have been compromised.

- Password cracking or guessing will be performed on a periodic or random basis during audit penetration tests involving 3rd party companies. If a password is guessed or cracked during one of these scans, the user will be required to change it immediately.

10 Application Development Standards

Application developers must ensure their programs contain the following security precautions.
Applications:

- Should support authentication of individual users, not groups.
- Should not store passwords in clear text or in any easily reversible form.
- Should provide role management functionality, such that one user can take over the functions of another without having to know the other's password.
- Should support TACACS+ , RADIUS and/or X.509 with LDAP security retrieval, wherever possible.

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.